ITSAILOR

Privacy Policy

Effective 25 October 2026. Current version: https://www.itsailor.io/legal/privacy

We collect what we need to answer you, run our tools and deliver what you buy. We do not sell personal data and we run no advertising trackers.

01 Who is responsible

Michal Jatczak, a sole trader registered in Malta who trades as ITSailor, is the controller of the personal data described in this policy.

Level 1, Unit 60, Door No 63, Connecticlub Business Center, Triq Il-Ballut (Zona Industrijali, Mosta), MST 4001, Mosta, Malta. VAT MT32760411. Contact: privacy@itsailor.io.

We have not appointed a data protection officer, because our processing does not require one (GDPR Article 37).

This policy does not cover personal data we process for a client business as its processor: what a free tool reads from a tenant or subscription (section 7), the data our managed automation packages handle for a client, and data inside a client's systems during an engagement. For that data the client is the controller and its own privacy notice applies. If you write to us about it, we pass your request to the client without delay.

02 What we collect, why, and for how long

You visit the site
What we collect: IP address, browser, pages requested, time
Why: Running and securing the site, stopping abuse
Legal basis (GDPR): Legitimate interests, Art. 6(1)(f)
How long we keep it: 90 days. Rate-limit counters, which cap how often a form, sign-in, checkout or download can be used and are keyed to your IP address or, where a form sends email, to your email address or a code made from it, expire on their own within three hours

---

You accept analytics
What we collect: Pages visited and the time of each view, with identifiers removed and query strings cut to campaign tags; the domain of the site you came from; country, region and city, which Vercel derives from your IP address; browser, operating system and device type; a hash Vercel derives from the request to count visitors. No cookies, no cross-site tracking
Why: Seeing which pages and tools are useful
Legal basis (GDPR): Consent, Art. 6(1)(a)
How long we keep it: The hash is discarded after 24 hours. The page-view records are shown to us for 12 months; Vercel may keep them longer, at the latest until our agreement with it ends, when its terms require it to delete them

---

You use a free tool, or arrive from a tagged campaign link
What we collect: The event (a tool started, completed or failed, a SaaS Auditor scan completed, or an arrival from a campaign link), the tool or campaign label, the domain of the site you came from and the time. No cookie, no IP address and no identifier are stored
Why: Knowing whether the free tools work and which campaigns bring visitors
Legal basis (GDPR): Legitimate interests, Art. 6(1)(f)
How long we keep it: 24 months

You contact us
What we collect: Name, email, organisation, your message; your IP address, used only for a rate-limit counter that expires within three hours and is not stored with your message
Why: Replying to you, and counting requests in aggregate by the page, offer or campaign link they came from
Legal basis (GDPR): Legitimate interests
How long we keep it: 12 months after you contacted us; if we go on to work together, what the work needs moves to the engagement or order record below

---

You use a free tool or download
What we collect: Email (optionally name and company), the tool's inputs and results, what you downloaded
Why: Sending the report or download you asked for, answering your questions about it and, for one hour, limiting how many reports go to that address
Legal basis (GDPR): Legitimate interests
How long we keep it: 24 months after you used the tool or asked for the download

---

You set up renewal alerts in the SaaS Auditor
What we collect: Email, the renewals you chose to watch (vendor, date, amount), any Slack or Teams webhook you add
Why: Sending the alerts you asked for
Legal basis (GDPR): Legitimate interests
How long we keep it: Until you stop the alerts (reply to any alert)

You buy a workshop or eBook
What we collect: Name, email, company, billing address and country, VAT number, order details, payment reference; booking details for workshops
Why: Taking payment, delivering, invoicing
Legal basis (GDPR): Contract, Art. 6(1)(b); legal obligation for tax records, Art. 6(1)(c)
How long we keep it: 12 months after delivery; invoices and tax records 9 years after the transaction (10 years for sales declared through the EU One Stop Shop)

Your organisation orders licences
What we collect: Organisation details, VAT number and its VIES check, company registration number, Microsoft tenant ID and domain, products ordered, and the name and email of the person accepting the Microsoft Customer Agreement and of named administrators
Why: Placing and managing the order with Pax8 and Microsoft; tax records
Legal basis (GDPR): Contract; legitimate interests for named people who are not the buyer; legal obligation
How long we keep it: While the subscription runs, plus 12 months; tax records as above

---

You use the client panel
What we collect: Name, work email, password (stored hashed) or Microsoft sign-in identifiers, company, messages, tickets, project records, a log of actions in the panel
Why: Providing and securing your account and its services
Legal basis (GDPR): Contract
How long we keep it: While the account is open, plus 12 months

---

We work on an engagement
What we collect: Contact details of your staff, project communications and documents
Why: Delivering the engagement
Legal basis (GDPR): Contract; legitimate interests for your staff
How long we keep it: The engagement plus 12 months; tax records as above

---

You make a cookie choice
What we collect: Your choice, the consent form version, the language the banner was shown in, a random consent ID, your browser's user agent, the time and, when the hashing key is set, a salted hash of your IP address. The record never holds the address itself; the address is used only for a rate-limit counter that expires within three hours
Why: Proving consent, as GDPR requires
Legal basis (GDPR): Legal obligation, Art. 6(1)(c) with Art. 7(1)
How long we keep it: 24 months

Card details are handled by Stripe. We never see or store full card numbers.

Our legitimate interests are keeping the site secure and available, answering enquiries and requests you send us, delivering the free reports you ask for, fulfilling your organisation's orders and engagements (including contacting the people it names), and understanding in aggregate which content is useful and which pages and links bring enquiries. You can object to this processing at any time (section 6).

Do you have to give us data? Using the site, the tools and the contact form is voluntary; without the data we cannot send you a reply or a report. For a purchase, your name, email and billing details are needed to contract with you and invoice you. A licence order also needs the details Microsoft requires to activate a tenant and, for the reverse charge, a VAT number we can verify. Without them we cannot complete the order.

03 AI in our tools

- **Free-tool reports** are written by OpenAI from the tool's inputs and results. Your email address is not sent.
- **SaaS Auditor briefs** are written by Anthropic from aggregate figures only, with no names or other identities.
- **Contract upload in the SaaS Auditor:** if you choose to upload a contract, the whole PDF, including any names in it, is sent to Anthropic to extract its commercial terms. We do not store the file.
- **Managed automation packages:** AI steps send the text they work on to Mistral AI, on its EU endpoint. There we act for the client business you deal with, as its processor, under section 14 of our Terms of Service, and that business's privacy notice applies.

OpenAI's and Anthropic's terms state that API inputs are not used to train their models.

04 Who receives your data

Service providers who act on our instructions:

Stripe Payments Europe Ltd.
What for: Payments. Stripe is also an independent controller for its own fraud prevention, financial risk, AML and KYC obligations and product development
Where: Ireland

Microsoft Ireland Operations Limited (Microsoft 365)
What for: Our business email and files
Where: EU

Hetzner Online GmbH
What for: Our servers, databases and backups, including the automation server that runs managed automation packages
Where: Germany

Vercel, Inc.
What for: Website hosting, and analytics only if you accept it; the analytics is cookie-free and not used for advertising or cross-site profiling. Vercel is also an independent controller for the usage data its service generates
Where: Functions in Frankfurt; edge network and analytics outside the EEA

Cloudflare, Inc.
What for: DNS and a secure tunnel to our servers
Where: Global network

Resend (Plus Five Five, Inc.)
What for: Sending email: our own, and the email our managed automation packages send for a client
Where: United States

Upstash, Inc.
What for: Tool and security data: rate limits, sign-in state, scan results for up to 10 minutes, and Tenant Security Scorecard trend scores for up to 180 days
Where: Ireland

GitHub, Inc.
What for: Private repositories for client deliverables
Where: United States

OpenAI (API)
What for: Writing free-tool reports. API inputs are not used to train models
Where: Outside the EEA

Anthropic (Claude API)
What for: SaaS Auditor briefs from aggregate figures, and contract extraction when you upload a contract. API inputs are not used to train models
Where: Outside the EEA

Mistral AI
What for: AI steps in the managed automation packages, on its EU endpoint. Mistral is also an independent controller for the abuse monitoring its terms provide for
Where: EU and EFTA

Cal.com
What for: Booking calls and workshop sessions
Where: Outside the EEA

DocRaptor
What for: Producing eBook PDFs, which carry the buyer's email in the licence line
Where: Outside the EEA

Others who receive data for their own purposes:

- **Microsoft Ireland Operations Limited (licences):** Not our sub-processor. Licensor of the Microsoft licences you buy through us; it processes your tenant content as your provider, under its agreement with you.
- **Pax8, Inc.:** Not our sub-processor. Our distributor; it receives licence order details to fulfil your order, under its own terms. Your tenant data does not reach it.

- **Telegram Messenger Inc.:** Not our sub-processor. Messaging service that carries alerts and approval notices from our managed automation packages to the staff accounts that asked for them, and to us, under its own terms. It receives no personal data of a client's customers: a message carries a reference, a count or a status and a link to our own server.
- **Authorities, courts and professional advisers**, where the law requires it or to establish or defend legal claims.

The Subprocessor Register gives each provider's legal entity, processing location and transfer basis, and a dated log of changes. We give customers at least 30 days' notice by email before a new provider begins processing their personal data.

05 Transfers outside the EEA

Some providers above are based in, or process data in, the United States or elsewhere outside the EEA. For those transfers we rely on the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) and, where the provider is certified, the EU-US Data Privacy Framework (Decision (EU) 2023/1795), together with encryption in transit. You can ask for a copy of the clauses at privacy@itsailor.io.

Telegram, listed above among the recipients we do not instruct, offers its users no such safeguard. We therefore send it no personal data of anyone other than the person whose own account receives the message: an alert carries a reference, a count or a status and a link to our own server.

06 Your rights

You can ask us for a copy of your data, to correct it, to delete it, to restrict its use, or to receive it in a machine-readable format for yourself or another company. Where we rely on your consent, you can withdraw it at any time; this does not affect processing before the withdrawal.

Write to privacy@itsailor.io. We reply within one month, or within three months for complex requests, in which case we tell you within the first month. We may need to confirm your identity first. Exercising these rights is free.

> **Your right to object**
>
> You can object at any time, on grounds relating to your situation, to processing based on our legitimate interests. We then stop, unless we have compelling legitimate grounds or need the data to establish or defend legal claims. You can object to direct marketing at any time, without giving a reason.

You can complain to the Information and Data Protection Commissioner in Malta (idpc.org.mt) or to the supervisory authority in your EU country.

07 Free tools that connect to your tenant

The SaaS Auditor can read data from your Microsoft 365 or Google Workspace tenant, and the Offboarding Runbook and Leaver Check and the Tenant Security Scorecard from your Microsoft 365 tenant, after an administrator grants read-only consent, and the Cost Review for Azure can read one Azure subscription after an administrator gives our application the Reader role on it. For that data, your organisation is the controller and we are its processor, under the processor terms in section 14 of our Terms of Service. The consent or the role is your instruction, and you can revoke it at any time: in Microsoft Entra under Enterprise applications, in the Google Admin console under API controls, or by removing the role assignment in the Azure portal. The spend scan of an accounting system is the exception, described at the end of this section.

- **What we read:** directory and user data, sign-in activity, licences, roles and security settings, and for Google Workspace, third-party app grants and 2-step verification status. The exact permissions of each tool, and why each one is needed, are listed at itsailor.io/trust/scopes.

- **Google Workspace permissions:** `admin.directory.user.readonly`, `admin.directory.domain.readonly` and `admin.directory.user.security`. Google offers no read-only version of the last one. We use it only to read app grants and 2-step verification status, never to change or revoke anything.
- **What we keep:** the scan result for up to 10 minutes so the page can show it, encrypted with AES-256-GCM under a key our database provider does not hold; then it expires. For the Tenant Security Scorecard that result holds the verdicts, short evidence sentences (which can name a Conditional Access policy and say how many accounts it excludes), the tenant name and the Secure Score headline. We store no sign-in tokens. The Tenant Security Scorecard keeps nothing longer unless you tick Remember this result: then it keeps your score and the state of each control for 180 days, under a random code in your browser rather than your email, and unticking deletes it. Our logs replace directory identities with pseudonymous codes. If you leave your email on the scorecard result so a person can look at it, your email and the report's aggregate figures (score, band, and the counts of controls and critical gaps) are kept as described in section 2. Nothing is emailed to you automatically.
- **What the Offboarding Runbook and Leaver Check keeps:** for up to 10 minutes it holds the check result, so the page and the PDF record can show it. The result contains the user principal names, display names, device names and app names of the disabled accounts the check reads in depth (up to 40) and of the enabled accounts it flags, with the licence, role and consent details found for them. It is encrypted with AES-256-GCM under a key Upstash does not hold and stored by Upstash, Inc. in Ireland, inside the EEA (see the sub-processor register), and then expires; you can delete it sooner with Delete this scan now. We store no sign-in token. The check reads accounts and licences, last successful sign-in, the audit events that record when an account was disabled, delegated consents, app assignments, owned apps and groups, directory and PIM roles and Intune devices. It does not read mail, files, calendars, Teams content or security alerts. The runbook builder on the same page runs in your browser, and what you type into it is not sent to us. Our logs carry a keyed hash of the tenant ID and counts, never a name or an address.
- **What the Cost Review for Azure reads:** the cost, resources, Advisor recommendations and policy assignments of the one subscription, through the built-in Reader role, which reads and cannot change anything. Resource names and tags can contain a person's name. The result is shown on the page and not stored, and nothing is written to your Azure. If you leave your email for the report, its summary, which may not contain a subscription or resource identifier, is kept as described in section 2. Details are at itsailor.io/trust/scopes.
- **What we never do:** use tenant data to train AI models, sell it, or use it for advertising.
- **Google API Services User Data Policy.** ITSailor's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. We use Google Workspace data only to provide the audit you requested, transfer it only as needed to provide it or as required by law, and do not allow people to read it except with your consent, for security, to comply with the law, or in aggregated, de-identified form.
- **Spend scan of Xero or QuickBooks Online (SaaS Auditor), not yet available:** the SaaS Auditor does not offer this connection today; the spend scan reads a CSV export you upload. When it is switched on, this is how it works. For this read we are the controller, not your processor, because we decide what is read and kept; our basis is our legitimate interest in providing the scan you asked for (Art. 6(1)(f)), and you can object under section 6. With the permission you grant, we read up to 1,000 spend bank transactions from Xero or purchase transactions from QuickBooks Online into memory for the one request, and keep only the vendor summary (vendor, category and cost), encrypted with AES-256-GCM and stored by Upstash in Ireland for 10 minutes. A vendor can be a person you pay. We store no access or refresh token, and right after the read the scan ends its own access: it deletes the Xero connection, or revokes the QuickBooks token, which removes our permissions on your company. The people named in your transactions are not told individually, because nothing about them is kept beyond those 10 minutes (GDPR Article 14(5)(b)). The permissions are listed at itsailor.io/trust/scopes, and you can disconnect the app in Xero or QuickBooks at any time.

08 Cookies

Without your consent we store on your device only what a feature you use needs: sign-in, the free-tool scans, the inputs you give a tool and your consent choice. Vercel Web Analytics runs only if you accept it. Our own tool counters store nothing on your device. The Cookie Policy lists every cookie and storage key; you can change your choice at any time with "Cookie preferences" in the site footer.

09 Security

We protect personal data with measures suited to the risk, including encryption in transit, encrypted off-site backups, encrypted short-lived scan results, access limited to what each system and person needs, and regular updates. If a breach is likely to put your rights at risk, we notify the IDPC within 72 hours and, where the risk is high, tell you without undue delay.

10 Data we receive from others

When an organisation orders licences from us, it gives us the name and business email of the person who will accept the Microsoft Customer Agreement and of any administrator it names. Consulting clients may give us their staff's contact details. We use these only to fulfil the order or engagement, share licence order details with Pax8 and Microsoft, keep them as set out in section 2, and you have the rights in section 6. We tell you this at the latest when we first contact you.

11 Children

Our services are not aimed at children. We do not knowingly collect data from anyone under 16; if you think we have, contact us and we will delete it.

12 Automated decisions

We make no decisions based solely on automated processing that have legal or similarly significant effects on you. Scores and AI-written reports from our tools are advice for you to review.

13 Changes

We publish changes here with a new effective date, and email customers about material changes before they take effect.

14 Contact

privacy@itsailor.io. Post: Michal Jatczak, trading as ITSailor, Level 1, Unit 60, Door No 63, Connecticlub Business Center, Triq Il-Ballut (Zona Industrijali, Mosta), MST 4001, Mosta, Malta.